第54卷 第3期
2017年5月

北京大学学报(哲学社会科学版)
Journal of Peking University(Philosophy and Social Sciences)

Vol. 54, No. 3
May 2017

法 学 研 究

大数据时代个人信息保护的立法选择

张 平

(北京大学 法学院,北京 100871)

摘 要: 面对大数据洪流,个人信息的保护定位一直存在分歧,将数据信息作为一种积极趋利的权利还是一种消极保守的权利,在经济学、社会学和法学领域中有不同的反应。目前主要分为两大观点:一种认为大数据时代个人信息的利用应该受到严格控制,除传统隐私保护外,互联网环境下人们更需要一种"不被打扰的权利";另一种观点是大数据的开发和利用是互联网经济的必然趋势,各国视大数据为新的"黄金"资源,特别是人工智能的广泛应用,个人数据采集已成为常态,限制数据的利用会错失发展机会。应当从个人信息的法律属性出发,分析大数据时代利用数据信息的必然性及规范性,区分个人信息的人格权保护重点和个人信息数据库的财产权保护重点,以此来探讨大数据时代平衡产业发展与个人信息保护的适度立法。

关键词: 大数据;个人信息;隐私权

中图分类号:D 901 **文献标识码:**A **文章编号:**1000-5919(2017)03-0143-09

大数据时代飞速地向我们走来,以至于人们还没有认清楚它是"福"是"祸",就已经完全被大数据的洪流所推动,国家将大数据产业作为新的经济增长点,企业将大数据作为重要的商业资源。数据,已经渗透到每一个行业中,成为重要的生产因素。个性化精准广告推送已经成为主流的互联网广告模式。国家在大数据产业发展方面的各种利好政策也让数据产业方兴未艾①。

然而,作为大数据的主要贡献者——个人,尽管每天不胜其烦地接到骚扰电话、短信、邮件、莫名的上门服务,也已经接受了这样的现实,甚至也在享受大数据带来的好处,在出行、用餐、邮寄、上网搜索方面无不享受着精准服务带来的便利,而对于信息骚扰带来的烦恼,在无奈之下也只能期望采用技术措施加以屏蔽。

大数据带来的社会问题引起学术上的激烈争论:

经济学家们认为大数据已然成为国家之间、企业之间竞争的又一重要资源。大数据经济已经开始,"各种大量的数据进行不断地融合交汇再产生一些新数据,导致数据边际成本越来越低,边际效应越来越大,从而带来了新的经济形态"②。

社会学家担心大数据时代人们的幸福观会受到影响。"对于人类而言,遗忘一直是常态,记忆是例外,然而,由于数据技术与全球网络的发展,这种平衡已经被打破。如今,往事像刺青一样刺在我们的数字皮肤上,遗忘,已经变成了例外,而记忆却成了常态"③。《大数据取舍之

收稿日期:2017-03-30

作者简介:张平,女,辽宁沈阳人,北京大学法学院教授。

本文网站资料最后确认日期均为2017年3月30日。感谢北京大学法学院张金平博士生和北京航空航天大学法学院赵精武博士生为本文提供的数据资料。

① 2016年3月,国家大数据(贵州)综合试验区被批准。目标是通过3至5年的时间,培育一批大数据骨干企业,推动经济转型升级。

② 上海社会科学院信息研究所信息安全研究中心主任惠志斌在"数据开放与发展纵横谈"论坛上的发言,2016年,北京。

③ 维克多·迈尔-舍恩伯格:《删除:大数据取舍之道》,杭州:浙江人民出版社2013年版,前言。

道》的作者进一步认为:“没有忘却的全息记忆将给人类带来巨大的负担,人们必须小心谨慎从事,担心那些不妥当的行为被永久记录”,“遗忘并不是令人困扰的缺陷,而是一种足以救命的优势”,“生物性的遗忘正是这样一种极为简单又优雅的忘却方式”①。但是,大数据却记住了所有人的人生轨迹并且不厌其烦地给每个人提供精准需求的服务。

法学家从不同侧面有不同的观察,早期的思路更多的是利用个人隐私、基本人权的保护制度来限制大数据应用与跨境数据传输,比如 WTO/GATS、OECD、APEC、美国、英国、德国等,都通过制定相关法律来规制互联网或者电子商务中的隐私保护。近期受技术与产业的影响,立法者意识到大数据的采集和流转已成不可阻挡之势,法律的责任是在维护基本权利之上考虑如何促进产业发展,以美国为代表的国家开始把个人信息的利用市场化。

市场化应用个人信息使其保护更趋复杂,电子商务利益之争的表象背后,尚存国家安全、信息安全、经济安全等多个深层次问题,也正是在这样的背景下,各国在这一问题上的态度不尽相同,每个国家都站在本国立场上进行立法选择。

一、个人信息的法律属性讨论

我国现阶段涉及个人信息保护的法律渊源基本上来自对隐私权的保护。但是隐私和个人信息在概念上有很大不同。隐私的范围相对比较明确,凡是个人不愿意公开披露且不涉及公共利益的部分都可以成为个人隐私,出于对人格利益特殊保护的需要,隐私权是一种消极的、防御性的权利,其属性更是一种人身权,尽管贩卖他人隐私内容同样可以营利(不论是本人还是他人),隐私的财产属性还是不被认可。

个人信息保护较隐私权而言,需要考虑的价值维度更为多元,包括人格权、数据经济的发展、国家安全等。在大数据时代,隐私权与个人信息保护之间有着不同的保护内涵以及法律定位,但是,在一些国际组织规则和国家立法名称上仍然将“隐私”与“个人信息”通用,在全球电子商务环境下,实务界多以隐私政策合规来考量个人信息的保护水平,网站上的隐私保护协议以及各类隐私认证机构也都包含个人信息保护的内容,从广义上说,特别是涉及电子商务数据处理时两者有同一所指的倾向。

目前对个人信息的定义有诸多争议,但基本共识是:个人信息是指能够单一或者组合之后识别特定个人的一切信息,包括姓名、年龄、体重、档案、医疗记录、收入、家庭住址、电话号码、汽车发动机号、电脑序列号,甚至是行走路线、消费习惯、上网浏览记录等。个人信息最基本的特征是具有识别性,不论是直接的还是间接的、单一信息抑或组合信息,只要能够判断出特定个人的信息即认为属于个人信息;个人信息的主体为个人,即为自然人,社会组织、法人的数据信息不属于个人信息范畴;个人信息包含个人隐私,兼有人格权与财产权双重属性。

关于个人信息的法律属性目前学界有三种主流学说:

一是隐私权客体说,该学说认为个人信息即“数据隐私”(Data Privacy)属于隐私利益中的内容,数据隐私强调对个人数据的控制与利用。此种保护模式主要是基于美国法语境下的“隐私”概念,作为隐私权进行保护,这一观念也为我国一些学者所支持②。

二是人格权客体说,该学说主要为大陆法系国家如德国、法国所采用,认为在人格权框架下对个人信息进行保护是有效的③。“个人信息的收集、处理或利用直接关系到个人信息本人的人格尊严”④,将个人信息置放在人格权框架下进行保

① 维克多·迈尔-舍恩伯格:《删除:大数据取舍之道》,第 142—149 页。
② 陈红:《个人信息保护的法律问题研究》,《浙江学刊》2008 年第 3 期。
③ 王利明:《论个人信息权的法律保护——以个人信息权与隐私权的界分为中心》,《现代法学》2013 年第 4 期;王秀哲:《信息社会个人咨询隐私权的法保护》,《徐州师范大学学报》2005 年第 5 期。
④ 齐爱民:《个人信息保护法研究》,《河北法学》2008 年第 4 期。

护比较合适。

三是所有权客体说,该学说认为个人信息是一种财产利益,个人对数据享有占有、使用、收益、处分的权利①。该学说主要代表以美国波斯纳法官的隐私经济学理论为核心,也被我国一些学者所主张,认为应当对个人信息采取财产权保护②。

除此之外,还有资料权客体说③、法益说④等。

笔者认为上述几种学说均有其合理性,个人信息本质上是人格主体的自由表达,个人信息虽有直接和间接之分,但固定指向具体的个人使得信息具有特定的人格属性在学界并无争议。个人信息所具有的财产属性也已成为现实,信息在特定的情形下进行交易并流通是未来大数据产业的基础。但是上述学说也有其局限性,即将个人信息的财产权与个人信息数据库的财产权混同为一个概念,实际上大数据产业基于的数据是海量数据的集合,绝非单个个人的几条信息,单纯的个人信息不足以称为资源(名人的信息除外),只有大数据才有可挖掘的价值和不断衍生出新的商业服务模式的可能。现代意义上的个人信息数据库实际上更有保护的必要,商家的资金投入、数据收集与处理、数据的利用规则、利益分配等方面更应当是个人信息立法的内容之一。所以,笔者认为在立法考量上:个人信息的属性应当以人格属性为主导,财产价值依附于人格属性之下,保护人格权是第一位的,财产权是第二位的;而商家的个人信息数据库则应当以财产权属性为主导,经过收集、加工、处理之后的个人信息数据库其权利属性发生了变化,无论是政府、社会组织还是商人收集到的个人信息在经过去识别化后即让这些数据库转变为具有财产属性的数据财富,应当鼓励数据库的市场化运行,而这些数据库的主体也发生了变化,由个体数据主体变为投资人数据主体。

二、欧、美个人信息保护立法模式分析

在个人信息利用上,欧盟与美国可谓是消极限制和积极利用的典范,二者采取不同的立法保护模式。

欧盟对个人信息的保护比较保守,从价值属性上看,更注重个人数据隐私的人权特性与社会价值,以人格保护为重点,采取的是一种全方位国家立法模式。从横向上看,其范围包括一般性使用和特殊性使用,基本上涵盖了所有数据主体,包括公务机关和非公务机关的使用行为都纳入了监管范围内;从纵向看,其行为包括数据的收集、使用、储存和删除等各个环节,从主体到行为的横纵结合保证了数据的全方位保护。在执行体制上,欧盟采取了以国家公权力监督为主导的自上而下的模式,设立国家数据保护机构—欧盟数据保护委员会(European Data Protection Board, EDPB),负责对企业或组织的数据处理进行监督,对违法数据收集行为进行审计、调查、处罚和制裁,要求处理数据的企业或组织配备专门的数据保护专员(Data Protection Officer, DPO),专员需接受欧盟数据保护委员会的管理,在企业或组织发生个人数据操作违规时其需承担相应的责任。在跨境数据传输问题上,欧盟强调“No privacy, No trade”,在国际贸易中特别强调隐私权保护。

美国对个人信息采取了积极利用的态势,无论是学界还是实务界都有市场化的取向。美国更关注个人数据的经济特性和个人价值,采取分散立法模式,按照行业进行联邦立法(如通讯、金融、教育、保险和儿童上网隐私等),没有专门的法典就该问题进行规制。在监管上采取行业自律的模式,这种做法更符合高效、便捷、与时俱进的市场需求。美国是信息技术最为发达的国家,其

---

① 刘德良:《个人信息的财产权保护》,《法学研究》2007年第3期;汤擎:《试论个人数据与相关法律的关系》,《华东政法学院学报》2000年第5期。

② 刘德良:《个人信息的财产权保护》,《法学研究》2007年第3期。

③ 张素华:《个人信息商业运用的法律保护》,《苏州大学学报》2005年第2期。

④ 王晓芬:《个人信息的法律属性及私权保护模式探究》,《河南财经政法大学学报》2016年第5期。

电子商务的发展居世界首位,在资料收集、信息处理上具有强大的优势,其在数据跨国流通中获益最大,是全球最大的数据进口国与数据出口国,故而从产业利益出发采取较为宽松的立法保护。在执行机制上,美国奉行数据使用者自律与个人自力救济相结合原则,以市场为主导、以行业自治为中心的数据隐私政策,尽量减少政府的干预,但是近年来,联邦贸易委员会(FTC)以及联邦通信委员会(FCC)也进行了大量的涉及个人信息保护的行政查处,由此可见在鼓励自律自治前提下,政府也进行了适当的介入。

正是由于上述差别,欧盟与美国在个人数据保护和利用上不断产生分歧。1998 年,美国开始与欧盟就隐私保护的"安全港"原则(Safe Harbor Principles)进行协商,以保证数据的跨界流动。2000 年 7 月,欧盟正式同意了美国商务部提出的"国际安全港隐私权原则",双方签订了所谓的"安全港"协议,该协议旨在达到欧盟所规定的个人数据信息保护的"适当性"程度,使公司或组织在满足"适当保护"标准时畅通数据信息的传输。该协议包括通知、选择、转送、安全、资料完整、渠道和执行等七项原则,在内容上比 1998 年公布的原则更为严格,充分体现了美欧在数据保护和数据传输方面的斗争与妥协。

"安全港"协议要求所有签字的公司或组织对其收集信息的种类、使用的目的以及在可能透露给的第三方信息时应当向"个人"提供"清晰和明显"的通知。如果信息准备披露给第三方或者用于不相关的目的,应当有渠道使得"个人"可以明示选择是否拒绝对其信息的收集。对于敏感信息的收集,必须经过"个人"明确表示同意。只有那些参加"安全港"或者签署保护数据合同的第三方,才可以接收传输的数据。参加的公司或组织必须保证"个人"可以获知有关他们的任何信息,并有机会改正、修改或者删除不准确的信息①。"安全港"协议折中处理了美国和欧盟之间隐私保护利益平衡,有利于美国公司一揽子解决在欧洲的数据业务,加入"安全港"协议的美国公司可不用逐个经"个人"授权而进行数据转移。

2016 年 5 月,欧盟实施更为严格的《一般数据保护法》(The EU General Data Protection Regulation, GDPR)。该法规定:获取、处理他人的个人信息的"控制者"需要得到"个人"的明确同意,这种同意必须是自愿并且随时可以撤回。这部法律落实了之前由司法判例确立的"被遗忘权"的合法性②。"被遗忘权"的判例曾经引起许多争议,最大的争议点是这一判决会严重影响数据产业的发展。美国作为数据产业的强国以及作为互联网基础技术的控制者,不希望被欧盟法律所牵制,更不希望看到其他国家效仿欧盟法律。在欧盟率先废除了实施多年的美欧数据传输"安全港协议"之后,美国不得不再与欧盟签订新的"隐私盾协议"(Privacy Shield)③,以企业自愿的方式与欧洲妥协。隐私盾协议将欧美双方产业利益的争议掩盖在了协议之下,对其他国家则另当别论。"隐私盾协议"与之前的"安全港协议"最重要的差别是更加严格了个人信息再次转移给第三方的责任,对于在"隐私盾协议"下认证的那些机构再把数据转移给第三方时,无论第三方是否也是"隐私盾协议"认证的机构,必须把数据处理活动限制在数据主体同意的条款范围内,并使第三方遵守"隐私盾协议"认证机构要求承诺遵守的标准。

2017 年 3 月,美国参、众两院先后宣布废除联邦通信委员会(FCC)颁布的网络用户隐私权保护法案,这意味着互联网公司可以不顾及网络用户的感受,肆意收集和出售用户的浏览记录、健康数据及其他上网信息。美国互联网隐私保护政策正在发生急剧变化,这不仅激化了美国国内的互

---

① 信息来源于美欧安全港列表,http://2016.export.gov/safeharbor/index.asp。

② 判决书参见:http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0131&qid=1461468702602&from=EN。

③ 2016 年 2 月,欧盟委员会和美国商务部联合宣布他们达成了新的数据跨大西洋转移的协议——《欧美隐私盾协议》(EU-US Privacy Shield)。隐私盾协议原文参见 http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_eu-us_privacy_shield_en.pdf。

联网公司与消费者的对立,更会导致美欧个人信息保护战的进一步升级。

美国与欧盟在个人数据保护与跨境传输上的规则充分体现了国家利益和产业利益之争,其他国家无法完全效仿,现实情况是:日本、韩国和我国的港澳台地区都小心翼翼地采取贸易保护主义的做法,防止个人信息被无限制地传输和利用。

三、我国个人信息保护的法律追溯

我国对个人信息的保护散见于不同法律中,多以间接保护方式加以规定。我国《宪法》规定:"国家尊重和保障人权""公民的人格尊严不受侵犯""公民享有通信自由和通信秘密的权利""公民住宅不受侵犯"等;《民法通则》在人身权部分规定:"公民的人格尊严受法律保护";《刑法》规定:"非法搜查他人身体、住宅,或者非法侵入他人住宅""侵犯公民通信自由"等为犯罪行为;《民事诉讼法》规定:"对涉及个人隐私的案件应当不公开审理";《刑事诉讼法》规定"涉及个人隐私的案件不公开审理"。此外,在《妇女权益保护法》《执业医师法》《邮政法》《商业银行法》《律师法》《档案法》等也有间接规定。

我国法律中也有对个人信息保护问题进行的直接规定。《刑法》修正案(九)第二百八十六条之一:"网络服务提供者不履行法律、行政法规规定的信息网络安全管理义务,经监管部门责令采取改正措施而拒不改正,有下列情形之一的,处三年以下有期徒刑、拘役或者管制,并处或者单处罚金:(一)致使违法信息大量传播的;(二)致使用户信息泄露,造成严重后果的;(三)致使刑事案件证据灭失,情节严重的;(四)有其他严重情节的。

单位犯前款罪的,对单位判处罚金,并对其直接负责的主管人员和其他直接责任人员,依照前款的规定处罚。

有前两款行为,同时构成其他犯罪的,依照处罚较重的规定定罪处罚。"

《护照法》《身份证法》《消费者权益保护法》都有对"个人信息"保护的明确规定。2012 年 12 月 28 日全国人民代表大会常务委员会颁布了《关于加强网络信息保护的决定》。该《决定》提出:主管机关、网络服务提供者和其他企事业单位应当采取有效措施保护个人数据,该《决定》还确定了收集、使用个人数据的基本原则,要求相关主体明示收集、使用信息的目的、方式和范围,并经被收集者同意。① 2013 年 7 月 16 日工信部《电信和互联网用户个人信息保护规定》,强调电信业务经营者、互联网信息服务提供者在收集数据时必须遵守"知情同意原则",强化了有关机构的数据安全保障义务,并明确了相应的责任形态②。2017 年 3 月 15 日发布的《民法总则》特别规定了个人信息的保护,其第一百一十一条规定:"自然人的个人信息受法律保护。任何组织和个人需要获取他人个人信息的,应当依法取得并确保信息安全,不得非法收集、使用、加工、传输他人个人信息,不得非法买卖、提供或者公开他人个人信息。"此外,《民法总则》第一百二十七条规定:"法律对数据网络虚拟财产的保护有规定的,依照其规定。"这应当是最新的有关个人信息的立法动向,再一次表明我国在个人信息法律保护上更加倾向于对个体私权的保护。

相比于其他国家和我国港澳台地区,我国尚没有一部对个人信息保护的专门立法和行政执法机构,在个人信息被严重侵害的时候,借助于刑法和民法都不足以及时制裁侵害人和有效补偿被侵害人。面对个人数据泄露、滥用堪忧的情况,最高人民法院发布了《关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》司法解释,力争弥补成文法的滞后性③。而设立

---

① 《全国人民代表大会常务委员会关于加强网络信息保护的决定》第二条。http://www.npc.gov.cn/npc/xinwen/2012-12/29/content_1749526.htm。

② 工信部《电信和互联网用户个人信息保护规定》,http://www.miit.gov.cn/n11293472/n11293877/n16381515/n16381547/16389765.html。

③ 《最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》,http://www.chinacourt.org/law/detail/2014/08/id/147944.shtml。

一个统一的行政机构保护个人信息也是非常必要的。

四、积极利用抑或消极限制的考量

对个人信息保护呈现出的积极利用与消极保护越来越有相辅相成的态势。

(一)公法与私法的共同作用

在法学公私二元区分的背景下,学者对公法与私法的侧重点的认识有所不同。从公法角度出发的欧盟学者们多关注大数据对法律制度本身所带来冲击,以及数据制度对公权力行使及私权利保护所带来的影响。正如有学者提到“大数据技术的广泛应用实际上正重塑着整个法律体系运作于其中的社会空间,改变着大数据掌控者(包括国家和商业机构)与公民个人之间的权利关系,并创造出许多无须借助法律的社会控制方式,大数据技术使个人变得越来越透明,而权力行使者却变得越来越隐秘”①。可见,公法角度下的个人信息保护立法多侧重于对政府、公共机构收集公民的个人信息的限制问题。

从司法角度来看,美国学者们更多关注数据信息的权利属性,倾向于人格权属性的观点要求限制数据处理者对个人信息的无节制利用,倾向于财产权属性的观点则主张强化个人信息的商业化利用及增加人格权商业化利用的财产收益。

世界上多数国家以隐私权保护为原点展开其个人信息的法律保护,其救济路径由纯粹的事后救济(司法救济)转变为事前(行政救济与行业测评等)与事后配合的二元救济模式,其中反映出公法与私法共同作用的趋势。

(二)人身权与财产权双元保护

美国哈佛大学的 Lawrence Lessig 教授早在 20 世纪末就提出了数据市场化的主张,他认为纯粹的合同路径与侵权路径并不符合数据经济的需求,应当赋权解决。一旦数据作为财产被承认,数据使用者就会有动力与数据主体议价,在一定程度上会改变用户在数据市场持续被忽视的境地,使得所有者获得动力②。

观察最新的司法判决,目前涉及数据利用的司法判决仍多聚焦于是否侵犯隐私权问题上,数据财产化仅仅作为一种理论被提及③。分别强调人格权与财产权争议的背后所反映的是以人格尊严为核心的隐私权保护模式抑或是以实现经济目为起点的财产权保护模式的选择问题。我国同样有学者建议针对个人信息的自我利用,提倡个人信息财产权,将个人对信息的处分取得利益的可能性予以权利化,以此与人身权相区分,并纳入民法财产权利体系予以调整④。但是在诸多按照财产利益处理的案件中均无法有效分配所有被侵害个人的赔偿费用,商业机构利用个人数据获得的所谓“非法利益”具体到每一个人所得到的赔偿数额少得可怜(几条信息的价值),以至于“个人”少有动力通过司法途径主张财产权,倒是消费者权益保护机构或者是行政监督机构在接到投诉之后提起的诉讼很多,但多以对非法利用者处以罚款为最后的结果⑤。可见,简单的设计个人信息财产权保护制度很有可能形同虚设,而根据具体情况,分别予以个人信息人格权与个人信息数据库财产权双元保护更为符合价值取向和市场规律。

(三)产业利益之争

美欧在个人信息保护的立法分歧本质上是一种产业利益之争。正因为欧洲没有发达的互联网服务产业,故而以设立严格的隐私权或者个人信息保护为由限制美国的互联网企业(谷歌在欧洲法院败诉,让谷歌在提供搜索引擎服务时承担更

① 郑戈:《在鼓励创新与保护人权之间——法律如何回应大数据技术革新的挑战》,《探索与争鸣》2016 年第 7 期。

② 参见 Lawrence Lessig, Code and Other Laws of Cyberspace, Basic Books.(1999)。

③ 参见 Matthew K. Downing v. Globe Direct LLC.,以及朱某诉百度案:江苏省南京市中级人民法院民事判决书(2014)宁民终字第 5028 号。

④ 参见刘德良:《论个人信息的财产权保护》,北京:人民法院出版社 2008 年版。

⑤ 凤凰科技,AT&T 收 2500 万美元创纪录罚单:因泄露近 28 万客户数据,http://www.chinaz.com/news/2015/0409/397059.shtml。

严格的审查义务)①。

欧盟对侵犯个人数据的行为采取的处罚措施十分严格,包括禁令救济,对公司工作场所和数据处理设施的稽查和调查,数额巨大的罚款,以及对于特大违法行为的刑事责任处罚等。除此之外,欧盟数据保护机构对侵犯个人数据的公司予以曝光,增大惩戒力度。近年来,欧盟官方认为美国谷歌公司、苹果公司等搜索引擎与移动设备服务供应商通过提供服务非法获取、侵犯公民个人数据,曾多次表态要加强对有关企业的监管。而谷歌、苹果等企业也在对欧盟立法机构开展游说公关,以减轻可能面临的执法压力②,美国政府亦出面为其企业进行整体谈判以获得欧洲市场,在美国国内则通过出台一系列文件③,系统阐述了美国政府大数据战略,以政策与相关法案构建了其隐私权保护的基本框架,保持美国在大数据经济中处于领先地位。

(四)国家安全之争

法国大法官路易·儒瓦内在1977 年经济合作与发展组织(OECD)隐私大会上提到,“信息是一种实力,经济信息是经济实力的代表。信息具有经济价值,一国对于某些类别数据的存储和处理的能力能够赋予一国相对于他国的政治和技术上的优势。反过来,跨国数据转移却会导致一国国家主权的丧失”。④当前各国有关个人信息保护的立法尽管都在私法范围之内,但是涉及跨境数据传输时都必然要考虑到国家安全问题,各国都试图在跨境数据传输上采取双重标准,一方面自己尽可能抓取他国的数据,但又尽可能避免自己的数据外流,跨境数据传输问题看似是私法问题,其实涉及数据主权与数据资源的争夺,过分开放的数据流动政策显然不利于国家安全,这也是为何欧盟一直竭力主导欧美跨境数据流动的各类协议。欧美在个人数据保护方面的矛盾是欧美企业间的矛盾,归根到底还是国家数据主权与经济实力的斗争。这场较量将是一个持久战,谁在经济上最终战胜对方,谁就获得了主动权和更多的回旋余地。

五、个人信息保护的中国路径

(一)区分个人信息人格权与个人信息数据库财产权

在过分侧重人格化的欧洲保护模式以及强调个人信息商业化利用的美国模式之间,我国在立法取向上应当综合借鉴,特别是应当看到互联网产业和人工智能技术的发展,大数据应用无时无处不在,商业机构在将数据去识别化之后的再应用已不可控制,单个个人对其数据提出保护要求几乎不可能获得有效的财产权救济,在这种情况下,对个人信息的立法保护重点应放在个人基本人格权的保护以及加工过的个人信息数据库财产权的保护。个人信息保护的消极限制(仅限于人格权保护)与积极利用(鼓励财产权行使)本质上是多重因素作用的选择问题。当前大数据时代的个人信息生态系统及流转方式,显然无法适应新业态的发展需求,我们应当重新审视个人信息保护的规则及秩序,构建平衡产业发展与个人信息保护的新思路。借鉴欧盟和美国的经验,无论是采取信息财产权的积极利用还是人格权消极保护,这场战争背后的制度逻辑在于如何更好地将个人信息保护置于一部国家的法律体系中且需要与国家的政治、经济需求相契合,个人信息保护的

① 案件来源:http://www.36dsj.com/archives/18240。

② 李明:《“大数据时代”的美国隐私权保护制度》,《互联网金融与法律》2014 年第9 期。

③ 此处仅列出几份文件,其他可在白宫官方网站上搜索:1. Big Data: Seizing Opportunities, Preserving Values, Executive Office of the President,MAY2014。2. Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights,Executive Office of the President,May 2016。3. White House Office of Science and Technology Policy,Request for Information on the Future of Artificial Intelligence。

④ 参见 Statement of Louis Joinet, French Magistrate of Justice, Remarks before the Organization for Economic Cooperation and Development Symposium on Transborder Data Flows and the Protection of Privacy, in Vienna, Austria (Sept. 1977),http://law.emory.edu/elj/elj－online/volume－64/responses/data－nationalism－its－discontents.html。

立法初衷应当是:为避免大规模数据处理对个人的权益及自主性造成损害,首先应当保证个人的基本人格权,之后应当顺应技术与产业发展趋势,在个人信息去识别化后允许数据的再加工和利用,对于去识别化后的数据库给以财产权保护。

(二)禁止溯源制度

在个人信息的分类模式上应当重新考量。传统意义上的敏感与非敏感数据保护模式显然不符合大数据时代需求,个人信息应当区分为三个层次。首先是私人隐私信息,这部分为彰显自然人人格属性应当得到格外的关注和重视,例如犯罪记录、指纹信息,人脸识别等;其次是个人间接信息,需要经过分析加工工后可定位到个人,例如:购物信息、聊天记录、行走路线等。最后是加工信息①,这部分信息经过加工后很难识别出个人的信息,例如:大数据分析报告中将大量的原始信息脱敏处理形成的分类数据库,这部分信息很难与信息原始主体形成一一对应的关系,事实上,数据财产化与人格化争议的核心就在此类数据库上,数据库加工过程中原始数据主体多不知情,企业完全可以自我操控,但这些经过去识别化的数据企业也有技术能力还原,一旦还原又很容易识别出"个人",所以,法律当对这类数据库加工者苛以较为严苛的限制,禁止任意溯源。最新修订的日本《个人信息保护法》以匿名化为起点进行保护,匿名加工信息是指对不能识别特定个人的信息进行加工而且该加工过的个人信息也不能复原并追溯到个人②。我国个人信息保护应当以信息处理匿名化为基点重新构造,以数据的不可追溯为核心。

(三)国家设立行政监管机构以及商业机构设立隐私保护官制度

在监管体制上我国需要设立相应的行政执法机构。采用刑法、民法对个人信息保护都有实践上的局限性,对恶意侵权事件不能有效快速的制止,纵观各国立法,都有较强的行政监管体制发挥作用。日本设立个人数据保护委员会,韩国个人数据保护法中专门设置了纠纷调解委员会:通过简单的调解程序,可以采取停止侵害行为、恢复原状等相关措施。韩国个人信息纠纷调解委员会也可以解决损害赔偿问题,在一定程度上保证了纠纷解决的高效便捷③。美国的 FTC 有权制止企业的不公正和欺瞒行为,可以发出禁止、排除命令,制裁罚款等,欧盟的数据保护委员会,作为独立的行政机关监督个人信息保护的全过程。

商业机构的隐私风险并非产生于个人信息收集之初,多集中在使用环节,即使类似的信息因为使用场景的差异也会带来完全不同的结果,因此未来的信息立法应当更加重视信息使用阶段的监管。隐私保护官的设立对于商业机构非常必要。美国多数大型公司都设立首席隐私执行官,对公司的隐私保护执行政策进行评估。德国法律则要求其商业机构设立数据保护顾问。数据保护顾问的职责包括:对隐私事项检查、数据信息登记、监督数据处理活动等内容。数据保护顾问起到内部监管作用,同时德国联邦设立了数据监管机构,其主要监督《德国联邦数据保护法》以及其他涉及个人数据的使用和处理的法规的执行,对数据保护顾问进行监督,并在必要的时候提供援助。我国应当考虑设立个人信息保护官(隐私官)制度,完善商业机构的数据问责制。

(四)完善行业自律

在法律尚不完善之时,倡导行业自律有助于创造基本有序的产业环境,即使法律已经健全,倡导自律自治也非常便捷和高效。美国的非营利性网络隐私认证机构 TRUSTe、BBB online(Better Business Bureaus online)实行网络隐私认证计划,对企业的隐私保护随时进行测评。我国尚没有专门的行业自律规范,即使在《中国互联网行业自律公约》中也没有明确约定。为了增强我国互联网企业保护个人信息的意识,促进互联网企业遵守基本的法律规范和商业道德,引导互联网企业

① 有学者称其为衍生信息,参见杨立新:《民法总则草案对权利客体规定的重要价值》,http://www.legaldaily.com.cn/fxjy/content/2016-08/24/content_6776089.htm? node=83328。

② 《日本个人数据保护法》,资料来源与笔者与日本学者的学术交流文献(第 2 条第 9、10 款、第 36-39 条)。

③ 资料来源:http://koreanlii.or.kr/w/images/0/0e/KoreanDPAct2011.pdf article47,第 47 条(纠纷的调解)。

制定更加规范的个人信息保护政策,2014 年,北京大学法学院互联网法律中心以独立的民间学术机构发布了《互联网企业个人信息保护测评标准》(双语版),确立了互联网企业在个人信息处理(收集、使用、转移和删除)上应当遵循的基本原则:1. 知情同意原则(Principle of Informed Consent);2. 合法必要原则(Principle of Legality and Necessity);3. 目的正当原则(Principle of Valid Purposes);4. 质量保证原则(Principle of Quality Assurance);5. 用户参与原则(Principle of User Participation);6. 安全保障原则(Principle of Security)①。2015 年,互联网法律中心根据测评标准对 50 家国内外互联网企业的个人信息保护状况进行了产品体验和测评。从测评结果看,我国互联网企业对个人信息的整体保护处于中下水平,个别企业有政策无保护,有些企业甚至完全空白,连形式上的隐私政策也没有。个人信息保护是前所未有的新的法律概念,在立法不完善之时,行业自律的作用不可忽视。希望我国的行业机构尽早建立民间的监管机制。

大数据应用的立法规制越来越远离当年隐私保护的初衷,到了一个形式上是产业利益竞争、实质上是国家安全控制的新阶段。每个国家在立法上都“各揣心腹事”,立法者在个人信息保护和自由高效发展大数据产业之间必须做出智慧的选择。

The Legislative Choice of Personal Information Protection in the Age of Big Data

Zhang Ping

(*School of Law*, *Peking University*, *Beijing* 100871, *China*)

Abstract: There are diverse reactions from different social groups in the stream of big data. Should the protection of personal information be a right to be actively used or a right to be strictly restricted? There are two kinds of views among the jurists. One view is that the use of personal information should be strictly controlled in the age of big data. Besides the traditional privacy protection under the internet environment, people need a “not-to-be-disturbed right”. The other view is that the development and utilization of big data are the inevitable trend of the Internet economy. Various countries are competing for the resources of big data, especially for the widespread utilization of artificial intelligence. As the collection of personal data has become normal, too much restriction of the data utilization may cause a country to miss the opportunity of development. This article is intended to analyze the legal attributes of personal information, and the necessity and normalization of the data information utilization in the age of big data, and also to explore the appropriate legislation on personal information protection.

Key words: big data, personal information, privacy right

(责任编辑　　李　铄)

① 参见北京大学法学院互联网法律中心网站,http://www.pkunetlaw.cn/xm_list_all.aspx。